

On varieties of rings whose finite rings are determined by their¹ zero-divisor graphs

A.S. Kuzmina

*Altai State Pedagogical Academy, 55, Molodezhnaya st.,
Barnaul, 656031, Russian
akuzmina1@yandex.ru*

Yu.N. Maltsev

*Altai State Pedagogical Academy, 55, Molodezhnaya st.,
Barnaul, 656031, Russian
maltsevy@gmail.com*

Abstract

The zero-divisor graph $\Gamma(R)$ of an associative ring R is the graph whose vertices are all nonzero zero-divisors (one-sided and two-sided) of R , and two distinct vertices x and y are joined by an edge iff either $xy = 0$ or $yx = 0$.

In the present paper, we study some properties of ring varieties where every finite ring is uniquely determined by its zero-divisor graph.

Keywords: Zero-divisor graph; finite ring; variety of associative rings

AMS Subject Classification: 16R10, 16P10

1 Introduction

Throughout this paper, any ring R is associative (not necessarily commutative).

The zero-divisor graph $\Gamma(R)$ of a ring R is the graph whose vertices are all nonzero zero-divisors (one-sided and two-sided) of R , and two distinct vertices x and y are joined by an edge iff either $xy = 0$ or $yx = 0$ [10].

The notion of the zero-divisor graph of a commutative ring was introduced by I.Beck in [3]. In this paper, all elements of a ring are vertices of the graph. In [2], D.F.Anderson and P.S.Livingston introduced the zero-divisor graph whose vertices are nonzero zero-divisors of a ring. In [2], the authors studied the interplay between the ring-theoretic properties of a commutative ring R with unity and the graph-theory properties of $\Gamma(R)$. For a noncommutative ring the definition of zero-divisor graph was introduced in [10].

The question of when $\Gamma(R) \cong \Gamma(S)$ implies that $R \cong S$ is very interesting. For finite reduced rings and finite local rings this question has been investigated in [1]. (We note that ring R is called *reduced* if R has no nonzero nilpotent elements.) In this paper, we study varieties of rings, where $\Gamma(R) \cong \Gamma(S)$ implies $R \cong S$ for all finite rings R, S . Note that some results concerning such varieties have been proved in [6].

Firstly, we fix some notations. Let \mathbb{Z} be the set of integers, \mathbb{N} the set of natural numbers, $\mathbb{Z}[x]$ the polynomial ring over \mathbb{Z} . For each prime number p by $GF(p^n)$ we denote the Galois field with p^n elements. For each number n let \mathbb{Z}_n be the residue-class ring modulo n . The symbol $J(R)$ denotes the Jacobson radical of a ring R . We define a finite ring R with unity to be an *local ring* if the factor-ring $R/J(R)$ is a field.

For each prime number p let

$$N_{0,p^n} = \langle a; a^2 = 0, p^n a = 0 \rangle; \quad N_{p^2} = \langle a; a^2 = pa, p^2 a = 0 \rangle;$$

$$N_{p,p} = \left\{ \begin{pmatrix} 0 & a & b \\ 0 & 0 & a \\ 0 & 0 & 0 \end{pmatrix}; a, b \in GF(p) \right\};$$

$$A_p = \begin{pmatrix} GF(p) & GF(p) \\ 0 & 0 \end{pmatrix}; \quad A_p^0 = \begin{pmatrix} GF(p) & 0 \\ GF(p) & 0 \end{pmatrix}.$$

Let the additive group of a ring R be a direct sum of its nonzero subgroups A_i , $i = 1, \dots, n$ and $n \geq 2$, i.e. $R = A_1 \dot{+} \dots \dot{+} A_n$. If A_i is ideal of R for all i , then we say that the ring R is *decomposable* and write $R = A_1 \oplus \dots \oplus A_n$. A ring R is called *subdirectly irreducible* if the intersection of all its nonzero ideals is a nonzero ideal of R [5]. It is known that every ring is a subdirect sum of subdirectly irreducible rings [5]. The ring of $n \times n$ matrices over a ring R is denoted by $M_n(R)$. For all elements x, y of a ring R we put $[x, y] = xy - yx$.

For every set $X = \{x_1, x_2, \dots\}$ let $\mathbb{Z}\langle X \rangle = \mathbb{Z}\langle x_1, x_2, \dots \rangle$ be the free associative ring freely generated by the set X . For every $f(x_1, \dots, x_d) \in \mathbb{Z}\langle X \rangle$ the number

$$\min\{\deg(h) \mid \text{all nonzero monomials } h \text{ of } f\}$$

is called *the lower degree* of the polynomial $f(x_1, \dots, x_d)$. We say that an polynomial $f(x_1, \dots, x_d)$ is *essentially depending* on x_1, x_2, \dots, x_d if $f(0, x_2, \dots, x_d) = \dots = f(x_1, \dots, x_{d-1}, 0) = 0$.

Let \mathfrak{M} be a variety of associative rings. We denote by $T(\mathfrak{M})$ the T -ideal of all polynomial identities of \mathfrak{M} . For a set $\{f_i \mid i \in I\} \subseteq \mathbb{Z}\langle X \rangle$ by $\{f_i \mid i \in I\}^T$ denote the smallest T -ideal containing all f_i . Also, let $T(R)$ be the T -ideal of all polynomial identities satisfied by a ring R .

For all varieties \mathfrak{M} and \mathfrak{N} by $\mathfrak{M} \vee \mathfrak{N}$ denote the union of these varieties. Note that $T(\mathfrak{M} \vee \mathfrak{N}) = T(\mathfrak{M}) \cap T(\mathfrak{N})$. Put $\mathfrak{L}_{p_1, \dots, p_s} = \text{var } N_{0, p_1} \vee \dots \vee \text{var } N_{0, p_s}$, where p_1, \dots, p_s are prime numbers such that $p_i \neq p_j$ for $i \neq j$.

A finite ring R is called *critical*, if it does not belong to the variety generated by all its proper subrings and factor-rings [7]. We say that a variety \mathfrak{M} is *Cross* if the following conditions hold: (i) all rings of \mathfrak{M} are locally finite; (ii) the set of all critical rings in \mathfrak{M} is finite; (iii) $T(\mathfrak{M})$ has a finite basis. By [7], a variety of associative rings is Cross if and only if it is generated by a finite associative ring.

In this article, K_n will denote the complete graph on n vertices.

The aim of this paper is to prove the following theorems.

Theorem 1.1. *Suppose \mathfrak{M} is a variety of associative rings such that $xy + f(x, y) \in T(\mathfrak{M})$, where the lower degree of $f(x, y)$ is greater than 2. Then $\Gamma(R) \cong \Gamma(S)$ implies $R \cong S$ for all finite rings $R, S \in \mathfrak{M}$ if and only if $\mathfrak{M} \subseteq \mathfrak{L}_{p_1, \dots, p_s} \vee \text{var } \mathbb{Z}_p$ where p, p_1, \dots, p_s are prime numbers and $(p_i, p) \neq (3, 2)$ for $i \leq s$.*

Theorem 1.2. *Let \mathfrak{M} be a variety of associative rings such that $\mathbb{Z}_p \in \mathfrak{M}$ for some prime number p . Suppose $\Gamma(R) \cong \Gamma(S)$ implies $R \cong S$ for all finite rings $R, S \in \mathfrak{M}$. Then any subdirectly irreducible finite ring $A \in \mathfrak{M}$ satisfies one of the following conditions:*

- (1) $A \cong \mathbb{Z}_p$;
- (2) A is a nilpotent ring and $q^2 A = (0)$ for some prime number q .

Theorem 1.3. *Let \mathfrak{M} be a variety of associative rings such that $\mathbb{Z}_2 \in \mathfrak{M}$ and $\Gamma(R) \cong \Gamma(S)$ implies $R \cong S$ for all finite rings $R, S \in \mathfrak{M}$. Then any subdirectly irreducible finite ring $A \in \mathfrak{M}$ of order 2^t ($t > 0$) satisfies one of the following conditions:*

- (1) $A \cong \mathbb{Z}_2$;
- (2) A is a nilpotent commutative ring and $2x = 0, x^2 = 0$ for each $x \in A$.

Note that Theorem 1.2 strengthens the main result of [6].

2 The auxiliary results

To prove the main theorems, we need several supplementary results. Propositions 2.1–2.5 were proved in [6]. These statements will be used in what follows.

By Tarski's theorem (see [11]), any nontrivial variety of rings contains either $\text{var } \mathbb{Z}_p$, or $\text{var } N_{0, p}$, where p is some prime number. The question of when $\Gamma(R) \cong \Gamma(S)$ implies $R \cong S$ for all finite rings R, S in $\text{var } \mathbb{Z}_p$ ($\text{var } N_{0, p}$) is interesting. The following proposition answers this question.

Proposition 2.1. *Suppose \mathfrak{M} is either $\text{var } \mathbb{Z}_p$, or $\text{var } N_{0, p}$, where p is some prime number. Then $\Gamma(R) \cong \Gamma(S)$ implies $R \cong S$ for all finite rings $R, S \in \mathfrak{M}$ (see [6]).*

Proposition 2.2. *Let \mathfrak{M} be a variety of rings such that $\Gamma(R) \cong \Gamma(S)$ implies $R \cong S$ for all finite rings $R, S \in \mathfrak{M}$. Then the following conditions hold:*

- (1) if $\mathbb{Z}_p \in \mathfrak{M}$ for some prime number p , then \mathfrak{M} does not contain any field with the exception of \mathbb{Z}_p ;
- (2) either $x^t \in T(\mathfrak{M})$, where $t > 0$, or $\mathbb{Z}_p \in \mathfrak{M}$ for some prime number p ;
- (3) if a local ring R is in \mathfrak{M} , then it is a field;
- (4) if $n \geq 2$, then $N_{0, p^n} \notin \mathfrak{M}$ for each prime number p (see [6]).

Proposition 2.3. Let p_1, \dots, p_s be prime numbers such that $p_i \neq p_j$ for $i \neq j$. Then $\Gamma(R) \cong \Gamma(S)$ implies $R \cong S$ for all finite rings $R, S \in \mathfrak{L}_{p_1, \dots, p_s}$ (see [6]).

Corollary 2.1. Let R be a finite ring. Then $\Gamma(R) = K_2$ iff R is isomorphic to one of the following rings:

$$N_{0,3}, \mathbb{Z}_9, \mathbb{Z}_3[x]/(x^2), \mathbb{Z}_2 \oplus \mathbb{Z}_2 \text{ (see [6])}.$$

Proposition 2.4. Suppose $\mathfrak{M} = \mathfrak{L}_{p_1, \dots, p_s} \vee \text{var } \mathbb{Z}_p$, where p, p_1, \dots, p_s are prime numbers such that $p_i \neq p_j$ for $i \neq j$ (p may be equal to p_i for some i). Then $\Gamma(R) \cong \Gamma(S)$ implies $R \cong S$ for all finite rings $R, S \in \mathfrak{M}$ iff $(p_i, p) \neq (3, 2)$ for $i \leq s$ (see [6]).

Proposition 2.5. For every prime number p

$$\Gamma(N_{p^2}) = \Gamma(N_{p,p}) = \Gamma(A_p) = \Gamma(A_p^0) = \Gamma(N_{0,p} \oplus \mathbb{Z}_p)$$

(see [6]).

Corollary 2.2. Suppose \mathfrak{M} is a variety of rings such that $\Gamma(R) \cong \Gamma(S)$ implies $R \cong S$ for all finite rings $R, S \in \mathfrak{M}$. Then $A_p, A_p^0 \notin \mathfrak{M}$ for each prime number p (see [6]).

Corollary 2.3. Suppose \mathfrak{M} is a variety of rings such that $\Gamma(R) \cong \Gamma(S)$ implies $R \cong S$ for all finite rings $R, S \in \mathfrak{M}$. If $\mathbb{Z}_p \in \mathfrak{M}$ for some prime number p , then $N_{p,p} \notin \mathfrak{M}$ (see [6]).

Corollary 2.4. Suppose \mathfrak{M} is a variety of rings such that $\Gamma(R) \cong \Gamma(S)$ implies $R \cong S$ for all finite rings $R, S \in \mathfrak{M}$. Then $N_{q^2} \notin \mathfrak{M}$ for each odd prime number q (see [6]).

Before proving the main results, let us prove a number of supplementary results.

Proposition 2.6. Suppose \mathfrak{M} is a variety of rings such that $\Gamma(R) \cong \Gamma(S)$ implies $R \cong S$ for all finite rings $R, S \in \mathfrak{M}$. Then $mx, dx + x^2g(x) \in T(\mathfrak{M})$, where $m \in \mathbb{N}$, $g(x) \in \mathbb{Z}[x]$, either $d = 1$, or $d = q_1q_2 \dots q_l$, and q_1, q_2, \dots, q_l are mutually different prime divisors of m .

Proof. By Proposition 2.2(4) we have $N_{0,4} \notin \mathfrak{M}$. Note that $T(N_{0,4}) = \{4x, xy\}^T$. Therefore $T(\mathfrak{M}) \not\subseteq \{xy\}^T$. It means that $T(\mathfrak{M})$ contains a polynomial $f(x) = kx + x^2\varphi(x)$, where k is some nonzero integer and $\varphi(x)$ is some polynomial in $\mathbb{Z}[x]$. Let $f(x) = kx + x^2\varphi(x) = kx + a_2x^2 + a_3x^3 + \dots + a_sx^s$, where $a_2, a_3, \dots, a_s \in \mathbb{Z}$, $s \geq 2$. Then

$$\begin{aligned} 2^s f(x) - f(2x) &= \\ &= (2^s - 2)kx + (2^s - 2^2)a_2x^2 + (2^s - 2^3)a_3x^3 + \dots + (2^s - 2^{s-1})a_{s-1}x^{s-1} = 0. \end{aligned}$$

Repeating the argument, we see that

$$(2^s - 2)(2^{s-1} - 2) \dots (2^2 - 2)kx \in T(\mathfrak{M}).$$

Thus the variety \mathfrak{M} satisfies the identities $mx = 0$ and $kx + x^2\varphi(x) = 0$, where $m = (2^s - 2)(2^{s-1} - 2) \dots (2^2 - 2)k$. We may assume that $k \geq 1$. Let $m = q_1^{\beta_1} q_2^{\beta_2} \dots q_t^{\beta_t}$, where q_1, q_2, \dots, q_t are prime numbers such that $q_i \neq q_j$ for $i \neq j$. By Proposition 2.2(4), we have $N_{0,q_i^2} \notin \mathfrak{M}$ for $i \leq t$. Therefore $T(\mathfrak{M}) \not\subseteq T(N_{0,q_i^2}) = \{q_i^2x, xy\}^T$, $i \leq t$. This implies that for every $i \leq t$ there exists a polynomial $\alpha_i x + x^2\psi_i(x)$ in $T(\mathfrak{M})$ such that $\alpha_i \in \mathbb{Z}$ and q_i^2 is not a divisor of α_i . Let d be the greatest common divisor of the numbers $\alpha_1, \alpha_2, \dots, \alpha_t, m$. We see that either $d = 1$, or $d = q_{i_1}q_{i_2} \dots q_{i_l}$, where q_1, q_2, \dots, q_l are mutually different prime divisors of m . If $d = 1$, then the proof is straightforward. Now let $d = q_{i_1}q_{i_2} \dots q_{i_l} \neq 1$. Note that $q_{i_\mu} \neq q_{i_\nu}$ for $\mu \neq \nu$. Further there exist integers v_1, v_2, \dots, v_t, v such that

$$\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_t v_t + mv = d.$$

Multiplying the identities

$$\alpha_1 x + x^2\psi_1(x) = 0, \dots, \alpha_t x + x^2\psi_t(x) = 0, mx = 0$$

by v_1, v_2, \dots, v_t, v respectively and summing them, we obtain $dx + x^2g(x) \in T(\mathfrak{M})$ for some $g(x) \in \mathbb{Z}[x]$. Finally, notice that every prime divisor of d is a divisor of m . This completes the proof. \square

Proposition 2.7. *Suppose \mathfrak{M} is a variety of rings such that $\Gamma(R) \cong \Gamma(S)$ implies $R \cong S$ for all finite rings $R, S \in \mathfrak{M}$. Then $T(\mathfrak{M})$ contains an identity of the form mx , where $m = q_1^{\beta_1} q_2^{\beta_2} \dots q_t^{\beta_t}$, $\beta_i \leq 3$ for all $i \leq t$, and q_1, q_2, \dots, q_t are prime numbers such that $q_i \neq q_j$ for $i \neq j$.*

Proof. From Proposition 2.6, $T(\mathfrak{M})$ contains an identity of the form mx for some integer m . Let F be the one-generated free ring in \mathfrak{M} . Suppose $m = q_1^{\beta_1} q_2^{\beta_2} \dots q_t^{\beta_t}$, where q_1, q_2, \dots, q_t are prime numbers such that $q_i \neq q_j$ for $i \neq j$. Therefore $F = \oplus_{i=1}^t A_i$, where A_i is a ideal of F and $q_i^{\beta_i} A_i = (0)$ for $i \leq t$.

We shall show that $\beta_i \leq 3$ for each i . Assume the contrary. Then we can assume without loss of generality that $\beta_1 \geq 4$. Since $2 \left\lfloor \frac{\beta_1}{2} \right\rfloor + 2 \geq \beta_1$, we have

$$\left(q_1^{\left\lfloor \frac{\beta_1}{2} \right\rfloor + 1} A_1 \right)^2 = q_1^{2 \left\lfloor \frac{\beta_1}{2} \right\rfloor + 2} A_1^2 = (0).$$

If the abelian group $\langle q_1^{\left\lfloor \frac{\beta_1}{2} \right\rfloor + 1} A_1, + \rangle$ contains a element of additive order q_1^δ for some $\delta \geq 2$, then the ring A_1 has a subring S such that $S \cong N_{0, q_1^2}$. This contradicts Proposition 2.2(4). Hence $q_1 \left(q_1^{\left\lfloor \frac{\beta_1}{2} \right\rfloor + 1} A_1 \right) = (0)$ and $\left\lfloor \frac{\beta_1}{2} \right\rfloor + 2 \geq \beta_1$. If $\beta_1 = 2a + 1$ for some natural number a , then we get $a + 2 \geq 2a + 1$. Hence $a \leq 1$ and $\beta_1 \leq 3$. Now assume that $\beta_1 = 2a$ for some natural number a . Therefore $(q_1^a A_1)^2 = (0)$. As before, it can be shown that $q_1 (q_1^a A_1) = (0)$. Thus $a + 1 \geq \beta_1$, i.e. $a \leq 1$ and $\beta_1 \leq 2$. So we have proved that $\beta_1 \leq 3$. This contradiction concludes the proof. \square

Proposition 2.8. *Suppose \mathfrak{M} is a variety of rings such that $\Gamma(R) \cong \Gamma(S)$ implies $R \cong S$ for all finite rings $R, S \in \mathfrak{M}$. For any finite ring $R \in \mathfrak{M}$ there exist prime numbers q_1, q_2, \dots, q_t such that $q_1^2 q_2^2 \dots q_t^2 R = (0)$ and $q_i \neq q_j$ for $i \neq j$.*

Proof. It follows from Propositions 2.6 and 2.7 that $T(\mathfrak{M})$ contains the polynomials $q_1^{\beta_1} q_2^{\beta_2} \dots q_t^{\beta_t} x$ and $q_{i_1} q_{i_2} \dots q_{i_l} x + x^2 g(x)$, where $g(x) \in \mathbb{Z}[x]$, q_1, q_2, \dots, q_t are prime numbers, $q_i \neq q_j$ for $i \neq j$, and $\beta_i \leq 3$ for each i . Therefore $q_1^3 q_2^3 \dots q_t^3 R = (0)$. We see that $R = \oplus_{i=1}^t R_i$, where $q_i^3 R_i = (0)$ for all $i \leq t$. Now let us prove that $q_1^2 R_1 = (0)$.

Assume that $q_1 \notin \{q_{i_1}, q_{i_2}, \dots, q_{i_l}\}$. In this case, there exist integers a, b such that $q_1^3 a + q_{i_1} q_{i_2} \dots q_{i_l} b = 1$. Hence R_1 satisfies the identity

$$q_1^3 a x + q_{i_1} q_{i_2} \dots q_{i_l} b x + b x^2 g(x) = x + x^2 h(x) = 0.$$

Thus $R_1 \cong \mathbb{Z}_{q_1} \oplus \dots \oplus \mathbb{Z}_{q_1}$ and $q_1 R_1 = (0)$ (see [5]).

Now assume that $q_1 \in \{q_{i_1}, q_{i_2}, \dots, q_{i_l}\}$. In the same way, it can be proved that R_1 satisfies a identity $f_1(x) = q_1 x + x^2 g_1(x) = 0$, where $g_1(x) \in \mathbb{Z}[x]$. For any nilpotent element $a \in R_1$ it follows that

$$0 = f_1(q_1 a) = q_1^2 a + q_1^2 a^2 g_2(a) = q_1^2 a(1 + a g_2(a)),$$

where $g_2(a) = g_1(q_1 a)$. Since the element a is nilpotent, we get $q_1^2 a = 0$. So for the case $R_1 = J(R_1)$, we have $q_1^2 R_1 = (0)$. Now we can assume that $R_1 \neq J(R_1)$. In this case, there exists a nonzero idempotent $e \in R_1$ such that $e + J(R)$ is a unity in the factor-ring $R_1/J(R_1)$ (see [4, p. 80, 94]). Therefore

$$R_1 = e R_1 e + e R_1 (1 - e) + (1 - e) R_1 e + (1 - e) R_1 (1 - e)$$

(see [4, p. 32]). Also, note that $e R_1 (1 - e) + (1 - e) R_1 e + (1 - e) R_1 (1 - e) \subseteq J(R_1)$ and $q_1^2 J(R_1) = (0)$. We shall show that $q_1^2 e = 0$. By Wilson's theorem (see [12]), it follows that $e R_1 e = Q + N$, where Q is a direct sum of matrix rings over Galois rings, N is a (Q, Q) -bimodule such that $N \subseteq J(R_1)$. Let $Q = \oplus_{i=1}^m M_{k_i}(S_i)$, where S_i is a Galois ring for all $i \leq m$. Assume that $k_1 \geq 2$. In this case, the variety \mathfrak{M} contains the ring A_{q_1} . This contradicts Corollary 2.2. Therefore $k_1 = 1$. Similarly, it can be proved that $k_2 = \dots = k_m = 1$. This means that $Q = \oplus_{i=1}^m S_i$. It is known that every Galois ring is local. From Proposition 2.2(3), we have that S_i is a field for each i . Thus $q_1 Q = (0)$. It implies that $q_1 e = 0$. So $q_1^2 R_1 = (0)$. In the same way, we can prove that $q_i^2 R_i = (0)$ for $i \geq 2$. It shows that $q_1^2 q_2^2 \dots q_t^2 R = (0)$. This completes the proof. \square

3 The proofs of main results

Now we are in a position to prove our main theorems.

The proof of Theorem 1.1.

Suppose $\mathfrak{M} \subseteq \mathfrak{L}_{p_1, \dots, p_s} \vee \text{var } \mathbb{Z}_p$ and $(p_i, p) \neq (3, 2)$ for each $i \geq 1$. From Proposition 2.4, $\Gamma(R) \cong \Gamma(S)$ implies $R \cong S$ for all finite rings $R, S \in \mathfrak{M}$. Moreover, $x(1 - x^{p-1})y \in T(\mathfrak{M})$, i.e. \mathfrak{M} satisfies the identity $xy - x^p y = 0$.

Conversely, suppose $\Gamma(R) \cong \Gamma(S)$ implies $R \cong S$ for all finite rings $R, S \in \mathfrak{M}$ and $xy + f(x, y) \in T(\mathfrak{M})$, where the lower degree of $f(x, y)$ is greater than 2. By Proposition 2.6, we have that $T(\mathfrak{M})$ contains a polynomial $mx, q_1 q_2 \dots q_l x + x^2 g(x)$, where $m \in \mathbb{N}$, $g(x) \in \mathbb{Z}[x]$, q_1, q_2, \dots, q_l are prime numbers such that $q_i \neq q_j$ for $i \neq j$. From Lvov's theorem (see [7]), \mathfrak{M} is a Cross variety. Therefore it is generated by its critical rings.

Consider a critical ring $R \in \mathfrak{M}$. From Propositions 2.6 and 2.8, the ring R satisfies a identities $q_1 q_2 \dots q_l x + x^2 g(x)$ and $q^2 x = 0$, where $g(x) \in \mathbb{Z}[x]$, q, q_1, q_2, \dots, q_l are prime numbers such that $q_i \neq q_j$ for $i \neq j$. Hence for some $h(x) \in \mathbb{Z}[x]$ either $x + x^2 h(x) \in T(R)$, or $qx + x^2 h(x) \in T(R)$. In the first case, we have $R \cong \mathbb{Z}_q$ (see [5]). Now we can assume that the ring R satisfies the identity $qx + x^2 h(x) = 0$. Let us consider the following cases.

Case 1: $R = J(R)$. In this case, from the identity $xy + f(x, y) = 0$, we get $R^2 = (0)$. Since $qx + x^2 h(x) = 0$ is a identity of R , we have $qx = 0$ for each $x \in R$. Thus $R \in \text{var } N_{0,q}$.

Case 2: $J(R) = (0)$. From the Wedderburn – Artin theorem (see [4, p. 80]) and Corollary 2.2, it follows that $R \cong \mathbb{Z}_q$. Thus $R \in \text{var } \mathbb{Z}_q$.

Case 3: $(0) \neq J(R) \neq R$. As above (see Case 1), we have $qJ(R) = (0)$. Let $e^2 = e$ be an idempotent of the ring R such that $e + J(R)$ is a unity in the factor-ring $R/J(R)$. As before (see the proof of Proposition 2.8), we have $qe = 0$. So the ring R is a \mathbb{Z}_q -algebra. It means that R is isomorphic to one of the following algebras: $\begin{pmatrix} GF(q_1) & GF(q_2) \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} GF(q_1) & 0 \\ GF(q_2) & 0 \end{pmatrix}$, $\left\{ \begin{pmatrix} a & b \\ 0 & \sigma(a) \end{pmatrix}; a, b \in GF(q^n) \right\}$, $\begin{pmatrix} GF(q_1) & GF(q_3) \\ 0 & GF(q_2) \end{pmatrix}$, where $GF(q_1) \subseteq GF(q_3)$, $GF(q_2) \subseteq GF(q_3)$ and σ is an automorphism of the field $GF(q^n)$ such that $\sigma \neq 1$. Hence \mathfrak{M} contains either A_q (A_q^0) or a local ring. This contradicts Proposition 2.2(3) and Corollary 2.2. Thus Case 3 is impossible.

Theorem 1.1 is proved. \square

The proof of Theorem 1.2.

Let \mathfrak{M} be a variety of rings such that the following conditions hold: (i) $\Gamma(R_1) \cong \Gamma(R_2)$ implies $R_1 \cong R_2$ for all finite rings $R_1, R_2 \in \mathfrak{M}$; (ii) $\mathbb{Z}_p \in \mathfrak{M}$ for some prime number p . Consider a subdirectly irreducible finite ring R in \mathfrak{M} . From Theorem of [6], we have either $R \cong \mathbb{Z}_p$, or $R = J(R)$. If $R = J(R)$, then, from Proposition 2.8, it follows that $q^2 R = (0)$ for some prime number q .

The theorem is proved. \square

The proof of Theorem 1.3.

Let \mathfrak{M} be a variety of associative rings such that the following conditions hold: (i) $\mathbb{Z}_2 \in \mathfrak{M}$; (ii) $\Gamma(R_1) \cong \Gamma(R_2)$ implies $R_1 \cong R_2$ for all finite rings $R_1, R_2 \in \mathfrak{M}$. Suppose $R \in \mathfrak{M}$ is a subdirectly irreducible finite nonzero ring of order 2^t . From Theorem 1.2, it follows that either $R \cong \mathbb{Z}_2$, or $R^n = (0)$ and $p^2 R = (0)$ for some numbers $n > 1$ and p (p is prime). If $R \cong \mathbb{Z}_2$, then the proof is trivial. Assume that $R^n = (0)$ and $p^2 R = (0)$. Since $|R| = 2^t$, we have $p = 2$ and $4R = (0)$.

We shall show that $N_4 \notin \mathfrak{M}$. Assume the contrary. Then $N_4 \in \mathfrak{M}$. Therefore $N_{0,2} \oplus \mathbb{Z}_2 \in \mathfrak{M}$. From Proposition 2.5, we have $\Gamma(N_4) = \Gamma(N_{0,2} \oplus \mathbb{Z}_2)$. By assumption, $\Gamma(R_1) \cong \Gamma(R_2)$ implies $R_1 \cong R_2$ for all finite rings $R_1, R_2 \in \mathfrak{M}$. So we have a contradiction. Hence $N_4 \notin \mathfrak{M}$. This yields that there exists a polynomial $f(x_1, \dots, x_d)$ such that $f(x_1, \dots, x_d)$ is essentially depending on x_1, x_2, \dots, x_d and $f(x_1, \dots, x_d) \in T(\mathfrak{M}) \setminus T(N_4)$. We note that $T(N_4) = \{xyz, 4x, 2xy, 2x + x^2\}^T$. Therefore $d \leq 2$. Let us consider two cases.

Case 1: $d = 2$.

We can assume that the polynomial $f(x, y)$ has a form

$$f(x, y) = xy + \alpha[x, y] + 2\psi(x, y) + \varphi(x, y),$$

where $\alpha \in \mathbb{Z}$, $\psi(x, y), \varphi(x, y) \in \mathbb{Z}\langle x, y \rangle$ and the lower degree of $\varphi(x, y)$ is greater than 2. Substituting y for x in $f(x, y)$, we obtain $f(x, x) = x^2 + 2\beta x^2 + x^3\varphi_1(x)$ for some $\varphi_1(x) \in \mathbb{Z}[x]$. Clearly, $x^2 + 2\beta x^2 + x^3\varphi_1(x) \in T(\mathfrak{M})$. So the ring R satisfies the identities $4x = 0$ and $(1 + 2\beta)x^2 + x^3\varphi_1(x) = 0$. Further, there exist integers u, v such that $(1 + 2\beta)u + 4v = 1$. Therefore the ring R satisfies $x^2 = x^3\varphi_2(x)$ for some $\varphi_2(x) \in \mathbb{Z}[x]$. Since $R^n = (0)$, $x^2 = 0$ for each $x \in R$. From proposition 2.6, it follows that $T(\mathfrak{M})$ contains a polynomial of the form

$$q_1 q_2 \dots q_s x + x^2 g(x),$$

where $g(x) \in \mathbb{Z}[x]$, q_1, q_2, \dots, q_s are prime numbers, and $q_i \neq q_j$ for $i \neq j$. Assume that the numbers q_1, q_2, \dots, q_s are odd. In this case, there exist integers q, t such that $(q_1 q_2 \dots q_s)q + 4t = 1$. Since the ring R satisfies $q_1 q_2 \dots q_s x + x^2 g(x) = 0$ and $4x = 0$, the T -ideal $T(R)$ contains a polynomial $x - x^2 g_1(x)$ for some $g_1(x) \in \mathbb{Z}[x]$. It is clear that $R = (0)$. We have a contradiction. Thus $q_i = 2$ for some i . As above, it can be proved that R satisfies $2x + x^2 g_2(x) = 0$ for some $g_2(x) \in \mathbb{Z}[x]$. Since $x^2 = 0$ for every element $x \in R$, the polynomial $2x$ belongs to $T(R)$. Since $x^2 = 0$ for each $x \in R$, it is easily shown that the ring R satisfies the identity $xy + yx = 0$. We know that $a = -a$ for each $a \in R$. Therefore $xy - yx = 0$ for all $x, y \in R$, i.e. R is commutative. So R satisfies $x^2 = 0$, $xy = yx$, $x_1 \dots x_n = 0$, and $2x = 0$.

Case 2: $d = 1$.

In this case, we can assume that the polynomial $f(x, y)$ has a form

$$f(x) = \alpha x + \beta x^2 + x^3 f_1(x),$$

where $\alpha, \beta \in \mathbb{Z}$ and $f_1(x) \in \mathbb{Z}[x]$. Assume that α is odd. In this case, the ring R satisfies $x = x^2 h(x)$ for some $h(x) \in \mathbb{Z}[x]$. Since R is a nilpotent ring, we see that $R = (0)$. We have a contradiction. Therefore α is even. Let $\alpha = 2m$ for some $m \in \mathbb{N}$. Hence

$$f(x) = 2mx + \beta x^2 + x^3 f_1(x) = \gamma x^2 + m(x^2 + 2x) + x^3 f_1(x), \quad (1)$$

where $\gamma = \beta - m$. Clearly, $f(x) \in T(N_4)$ whenever γ is even. Since $f(x) \notin T(N_4)$, it follows that γ is odd. Hence there exist integers a, b such that $\gamma a + 4b = 1$. Combining the identities $4x = 0$ and (1), we see that the ring R satisfies

$$x^2 + m_1(x^2 + 2x) + x^3 \mu(x) = 0, \quad (2)$$

where $m_1 \in \mathbb{Z}$ and $\mu(x) \in \mathbb{Z}[x]$.

Assume that m_1 is even. Then we have

$$0 = 2x^2 + 2m_1(x^2 + 2x) + 2x^3 \mu(x) = 2x^2(1 + x\mu(x)),$$

because $4x = 0$ for each $x \in R$. Since R is nilpotent, $2x^2 = 0$ is an identity of R . From (2), it follows that $x^2 + x^3 \mu(x) = 0$ also is an identity of R . Hence $x^2 = 0$ for each $x \in R$. As above, using Proposition 2.6, we can prove that R satisfies an identity $2x + x^2 g_2(x) = 0$ for some $g_2(x) \in \mathbb{Z}[x]$. This implies that $2x = 0$ for any $x \in R$. So we have proved that R satisfies $x^2 = 0$, $xy = -yx = yx$, $x_1 \dots x_n = 0$, and $2x = 0$ whenever m_1 is even.

Now assume that m_1 is odd. Let $m = 2q + 1$, where $q \in \mathbb{N}$. In this case, $T(R)$ contains the identity

$$x^2 + (2q + 1)(x^2 + 2x) + x^3 \mu(x) = 0.$$

This identity can be represented in the form

$$2(q + 1)x^2 + 2x + x^3 \mu(x) = 0$$

since $4x = 0$ for each $x \in R$. Hence,

$$2x = -x^3 \mu(x)(1 + q_1 x)^{-1} \quad (3)$$

for each $x \in R$, where $q_1 = q + 1$. By Corollary 2.3, we have $N_{2,2} \notin \mathfrak{M}$. Consequently there exists a polynomial $F(x_1, \dots, x_w) \in T(\mathfrak{M}) \setminus T(N_{2,2})$ essentially depending on x_1, \dots, x_w . Obviously, $w \leq 2$. Assume that $w = 2$. In this case, $F(x, y)$ can be represented in the form

$$F(x, y) = xy + \alpha[x, y] + 2\Phi(x, y) + \Psi(x, y),$$

where $\Phi(x, y), \Psi(x, y) \in \mathbb{Z}\langle x, y \rangle$ and the lower degree of $\Psi(x, y)$ is greater than 2. From (3), it follows that

$$2\Phi(x, y) = -\Phi(x, y)^3 \mu(\Phi(x, y))(1 + q_1 \Phi(x, y))^{-1}.$$

In other words, the lower degree of $2\Phi(x, y)$ is greater than 2. Thus $F(x, y)$ can be represented in the form

$$F(x, y) = xy + \alpha[x, y] + \Psi'(x, y),$$

where $\Psi'(x, y) \in \mathbb{Z}\langle x, y \rangle$ and the lower degree of $\Psi'(x, y)$ is greater than 2. Substituting y for x in the identity $F(x, y) = 0$, we obtain an identity $x^2 = x^3\omega(x)$ for some $\omega(x) \in \mathbb{Z}[x]$. Since R is nilpotent, $x^2 = 0$ for every $x \in R$. From (3), we get the identity $2x = 0$. So R satisfies $x^2 = 0$, $xy = yx$, $x_1 \dots x_n = 0$, $2x = 0$ whenever $w = 2$. Now let us consider the case $w = 1$. The polynomial $F(x, y)$ can be represented in the form

$$F(x) = \alpha x + \beta x^2 + 2\lambda(x) + x^3 p(x),$$

where $\lambda(x), p(x) \in \mathbb{Z}[x]$, $\alpha, \beta \in \{0, 1\}$, and one of the numbers α, β is not equal to zero. If $\alpha = 1$ then R satisfies some identity of the form

$$(1 + 2k)x + x^2 \lambda'(x) = 0,$$

where $\lambda'(x) \in \mathbb{Z}[x]$. This means that $R = (0)$. We have a contradiction. Therefore $\alpha = 0$ and $\beta = 1$. Hence,

$$F(x) = x^2 + 2\lambda(x) + x^3 p(x).$$

Multiplying $F(x)$ by 2, we get the identity

$$2x^2(1 + xp(x)) = 0.$$

We see that $2x^2 = 0$. Let $\lambda(x) = a_1x + a_2x^2 + \dots + a_Nx^N$, where N, a_1, \dots, a_n are some integers. Consequently,

$$x^2 + 2a_1x + x^3 p(x) = 0$$

is an identity of R . If a_1 is even then R satisfies $x^2 + x^3 p(x) = 0$. In this case, $x^2 = 0$, $xy = yx$, $x_1 \dots x_n = 0$, $2x = 0$ are identities of R . Now assume that a_1 is odd. Then

$$x^2 + 2x + x^3 p(x) = 0$$

for each $x \in R$. From the identity (3), it follows that R satisfies some identity of the form $x^2 + x^3 p_1(x) = 0$. Thus $x^2 = 0$, $xy = yx$, $x_1 \dots x_n = 0$, $2x = 0$ are identities of R .

This completes the proof of Theorem 1.3. \square

References

- [1] Akbari S., Mohammadian A. On the zero-divisor graph of a commutative ring, *J. Algebra* 274 (2004) 847–855.
- [2] Anderson D.F., Livingston P.S. The Zero-Divisor Graph of a Commutative Ring, *J. Algebra* 217(2) (1999) 434–447.
- [3] Beck I. Coloring of Commutative Rings, *J. Algebra* 116 (1988) 208–226.
- [4] Elizarov V.P. Finite rings, Moscow, *Gelios-ARV*, 2006 (in Russian).
- [5] Jacobson N. Structure of rings, *AMS, Colloquium Publications*, Vol. XXXVII, 1956.
- [6] Kuzmina A.S. On some properties of ring varieties, where isomorphic zero-divisor graphs of finite rings give isomorphic rings, *Siberian Electronic Mathematical Reports* 8 (2011) 179–190 (in Russian).
- [7] Lvov I.V. On varieties of associative rings I, *Algebra i Logika* 12(3) (1973) 269–297.
- [8] Maltsev Yu.N. On critical algebras, *Algebra i Logika* 20(2) (1981) 155–165.

- [9] Maltsev Yu.N., Kuzmin E.N. A basis for the identities of the algebra of second-order matrices over finite field, *Algebra i Logika* 17(1) (1978) 28–32.
- [10] Redmond S.P. The zero-divisor graph of a noncommutative ring, *Int. J. Commut. rings* 1(4) (2002) 203 – 211.
- [11] Tarski A. Equationally complete rings and relation algebras, *Indag. Math.* 18 (1956) 39–46.
- [12] Wilson R. On the structure of finite rings, *Pacific J. Math.* 51(1) (1974) 317–325.